REMARKS

Claims 1-18 were examined by the Office, and in the Office Action of December 4, 2007 all claims are rejected. With this response no claims are amended, added or cancelled. Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

Claim Rejections Under § 102

In section 3, on page 2 of the Office Action, claims 1, 3-4, 7, 9-10, 13 and 15-16 are rejected under 35 U.S.C. § 102(e) as anticipated by Morgan (U.S Patent No. 6,968,459). Applicant respectfully submits that Morgan fails to disclose or suggest independent claim 1, because Morgan fails to disclose or suggest all of the limitations recited in claim 1. Applicant respectfully submits that Morgan at least fails to disclose or suggest at least one storage area in the storage circuit, in which storage area protected data relating to circuitry security are located, as recited in claim 1.

Claim 1, and the other independent claims, are directed to circuitry provided with a processor operable in at least two different modes, one first secure operating mode and one second unsecure operating mode. In the secure mode, the processor has access to security related data located in various memories located within the circuitry. The security data includes cryptographical keys and algorithms, software for booting the circuitry, secret data such as random numbers used as cryptographical key material, and/or application programs. The access to these security data, and the processing of them needs to be restricted, since an intruder with access to security data could manipulate a device, for example a mobile terminal, in which the circuitry of the present invention is implemented. When testing and/or debugging the terminal, access to the security data is not allowed. For this reason, the processor is placed in the unsecure operating mode, in which mode it is no longer given access to the security data.

The present invention advantageously enables the processor of the circuitry to execute non-verified software downloaded into the circuitry. This allows testing, debugging and servicing of the electronic device and its software without risking that a third party is given access to information which makes it possible to manipulate the security related components of the device so as to affect the security functions when in the secure environment.

Morgan is generally directed to a secure computing environment in which a computer automatically operates in a full-access data storage mode, in which all data written to the removable storage device is encrypted and a user is given access to the storage device if authorized, when it detects a secure removable storage device. Otherwise, the computer operates in a restricted access mode in which the user is unable to write to the removable storage device and is unable to access sensitive data. Security information is stored on the data storage device. This information is detected by the computer which then generates a cryptographic key from the security information which is related to the storage device. If the security information is not present on the removable storage device the computer automatically operates in a restricted access mode in which the user does not have access to sensitive data on the storage device and data cannot be written to the removable storage device. The security information is thus clearly connected to the access of the storage device, not to circuitry security as recited in claim 1.

On page 2 of the Office Action, the Office asserts that: "Morgan discloses at least one storage area in the storage circuit, in which storage area protected data relating to circuitry security are located" at column 1, lines 55 – 62. However, contrary to the assertions of the Office, Morgan does not disclose or suggest a storage area where protected data relating to circuitry security are located, as recited in claim 1. Instead, Morgan discloses a storage device with device-specific security information stored thereon, i.e. information regarding the accessibility of the storage device itself, while the present invention is referring to circuit security, i.e. to the e.g. computer not the storage area. Morgan only discloses that sensitive data of the organization and data stored on other devices are accessible when the computer is operating in full-access data storage mode. See Morgan column 1, lines 55-62.

Furthermore, Morgan does not disclose or suggest different processor operating modes, and does not disclose a mode in which the storage circuit access control means are arranged to prevent the processor from accessing the storage area in which protected data are located when a second processor operating mode is set, thereby enabling the processor to execute non-verified software downloaded into the circuitry, as recited in claim 1. Morgan does not provide any indication what so ever in the reference about enabling the processor to execute non-verified software downloaded into the circuitry. See Morgan Figure 2; Abstract. Instead, Morgan discloses that in restricted-access mode, i.e. when the storage device is not fully accessible, the storage manager configures the storage as a read only drive such that *the user* can read data from

the removable disk but cannot write data to the storage (or alternatively the user cannot read data from nor write data to the storage). See Morgan column 7, lines 8-16. In addition, the user is prevented from accessing non-sensitive data within the organization.

While, Morgan provides a number of modes which are all concerned with the protection mode of the storage, none of the modes are concerned with a protection mode of the operating mode of the processor. As described above, the processor in the present invention can be set in a secure and an unsecure mode. In the secure mode, the processor has access to security related data located in various memories located *within the circuitry*. When the processor is placed in the unsecure operating mode, it is no longer given access to the security data *within the circuitry*. In the reference the storage area is set in a secure mode such that when removed and moved to a different computer the storage area is still secured.

Therefore, for at least the reasons discussed above, claim 1 is not disclosed or suggested by Morgan.

Independent claims 7 and 13 contain limitations similar to those recited in claim 1, and therefore are not disclosed or suggested by Morgan at least for the reasons discussed above in relation to claim 1.

The claims depending from the above mentioned independent claims are not disclosed or suggested by Morgan at least in view of their dependencies.

Claim Rejections Under § 103

In section 7, on page 3 of the Office Action, claims 2, 6, 8, 12, 14 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Sato (U.S. Appl. Publ. No. 2001/0055980), and in section 10, on page 4 of the Office Action, claims 5, 11, and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Ishidera (US Patent 2002/0040442 A1).

Sato is directed to a multi-mode cellular phone terminal supporting a plurality of communication systems, which multi-mode cellular phone terminal comprises a system timer for switching over a plurality of clocks and counting different timings to support a plurality of communications system. Ishidera is directed to a software apparatus which executes processes of software with reduced power consumption at the time of operation on a battery and a recording medium. The apparatus determines whether power saving is needed or not.

The cited references fail to make up for the deficiencies in the teachings of Morgan identified above, and because all of the rejected claims ultimately depend from an independent claim, the claims are not disclosed or suggested by the cited references.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and such action is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge Deposit Account No. 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,

Date: 14 February 2006

Keith R. Obert
Attorney for the Applicant
Registration No. 58,051

KRO/kas
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
Telephone:(203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955